Guidance for Industry

Food Producers, Processors, Transporters, and Retailers: Food Security Preventive Measures Guidance

This guidance represents the Agency's current thinking on appropriate measures that can be taken by food establishments to minimize the risk of food being subjected to tampering or criminal or terrorist actions. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. This guidance is being issued in accordance with FDA's Good Guidance Practices regulation (21 CFR 10.115; 65 FR 56468; September 19, 2000).

This guidance is designed as an aid to operators of food establishments (i.e. firms that produce, process, store, repack, relabel, distribute, or transport food or food ingredients or that prepare or distribute food at retail). It identifies preventive measures that they can take to minimize the risk that food under their control will be subject to tampering or criminal or terrorist actions. It is relevant to all sectors of the food system (i.e., from farm-to-table), including farms, aquaculture facilities, fishing vessels, producers, transportation operations, processing facilities, packing facilities, warehouses, and retail and food-service establishments. Operators of food establishments are encouraged to review their current procedures and controls in light of the potential for tampering or criminal or terrorist actions and make appropriate improvements. This guidance is designed to focus operators sequentially on each segment of the farm-to-table system that is within their control, to minimize the risk of tampering or criminal or terrorist action at each segment. Implementing enhanced preventive measures requires the commitment of management and employees to be successful and, therefore, both should participate in their development and review.

This guidance is divided into seven sections that relate to individual components of a food establishment operation: management of food security; physical security; employees; computer systems; raw materials and packaging; operations; and finished products. It also covers security strategies and evaluation of the security system. Not all of the guidance contained in this document is appropriate or practical for every food establishment. Operators should review the guidance in each section that relates to a component of their operation, and assess which preventive measures are suitable for their operation. A process called Operational Risk Management (ORM) may also help operators prioritize the preventive measures that are most likely to have the greatest impact on reducing the risk of tampering or criminal or terrorist actions against food under their control (See: Food Safety and Security: Operational Risk Management Systems Approach, November 26, 2001; www.cfsan.fda.gov).

Food Establishment Operations:

Food establishment operators should consider:

- assigning responsibility for security to qualified individual(s);
- encouraging all staff to be alert to any signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering;
- alerting identified management about any findings (e.g., providing training, instituting a system of rewards, building into job performance standards);
- immediately investigating all information about suspicious activity;
- alerting local law enforcement about all suspected criminal activity;
- providing an appropriate level of supervision to all employees, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially new employees;
- conducting daily security checks of the premises for signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering.
- implementing procedures to ensure the security of incoming mail and packages (e.g., securing mailroom, visual or x-ray mail/package screening)

- inspecting incoming and outgoing vehicles for suspicious, inappropriate or unusual items or activity;
- restricting entry to the establishment (e.g., checking in and out at security or reception, requiring proof of identity; issuing visitors badges - collected upon departure);
- ensuring that there is a valid reason for the visit before providing access to the facility - beware of unsolicited visitors restricting access to food handling and storage areas (e.g., accompanying visitors, unless they are otherwise specifically authorized);
- restricting access to locker rooms;
- applying the above procedures to everyone, including contractors, supplier representatives, truck drivers, customers, couriers, third-party auditors, regulators, reporters, visitors, etc.;
- protecting perimeter access with fencing or other appropriate deterrent;
- securing doors (including freight loading doors), windows, roof openings/hatches, vent openings, trailer bodies, tanker trucks, railcars, and bulk storage tanks for liquids, solids, and compressed gases, to the extent possible (e.g., using locks, "jimmy plates," seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes]);
- using metal or metal-clad doors to the extent possible, especially when the facility is not in operation (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes);
- minimizing the number of entrances to restricted areas (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes);
- accounting for all keys to establishment;
- using security patrols (uniformed and/or plain-clothed) and video surveillance, where appropriate;
- minimizing places that could be used to hide temporarily intentional contaminants (e.g., minimizing nooks and crannies);
- providing adequate interior and exterior lighting, including emergency lighting;
- implementing a system of controlling vehicles authorized to park on the premises (e.g., using placards, decals, key cards, cypher locks);
- restricting access to the laboratory (e.g., using key cards or cypher locks [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes]);
- restricting laboratory materials to the laboratory, except as needed for sampling or other appropriate activities;
- restricting access (e.g., using locks, seals, alarms, key cards, cypher locks) to sensitive materials (e.g., reagents and bacterial, drug, and toxin positive controls);
- assigning responsibility for integrity of positive controls to a qualified individual;
- keeping track of reagents and positive controls;
- investigating missing reagents or positive controls or other irregularities outside a pre-determined normal range of variability immediately, and alerting local law enforcement about unresolved problems, when appropriate;
- securing storage areas for hazardous chemicals (e.g., using locks, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any state or local fire codes that may apply before making any changes]);
- limiting access to storage areas for hazardous chemicals (e.g., using key cards or cypher locks [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes]);
- keeping track of hazardous chemicals;
- investigating missing stock or other irregularities outside a pre-determined normal range of variation and alerting local law enforcement about unresolved problems;
- screening employees (e.g., obtaining and verifying work references, addresses, and phone numbers);
- checking immigration status with U.S. Immigration and Naturalization Service, when appropriate
- performing criminal background checks, including Federal Bureau of Investigation Watchlist (remember to consult any state or local laws that may apply to the performance of such checks);

- applying these procedures to all employees, to the extent possible, including seasonal, temporary, contract, and volunteer employees;
- knowing who is and who should be on premises, and where they should be located;
- keeping information updated;
- establishing a system of positive identification and recognition (e.g., issuing photo identification badges with individual control numbers, color coded by area of authorized access);
- collecting the retired identification badge when an employee is terminated, either voluntarily or involuntarily;
- limiting access so employees enter only those areas necessary for their job functions (e.g., using key cards or cypher locks to sensitive areas, color-coded uniforms [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes]);
- changing combinations and/or collecting the retired key card when an employee is terminated, either voluntarily or involuntarily, and additionally as needed to maintain security;
- reassessing levels of access for all employees periodically;
- restricting personal items allowed in establishment;
- preventing workers from bringing personal items (e.g., lunch containers, purses) into food handling areas;
- establishing policy and providing for regular inspection of contents of employee lockers (e.g., provide metal mesh lockers, company-issued locks), bags, and vehicles when on company property;
- providing food security training to all new employees, including information on how to prevent, detect, and respond to tampering or criminal or terrorist activity;
- providing periodic reminders of the importance of security procedures;
- ensuring employee buy-in (e.g., involving employees in food security planning, demonstrating the importance of security procedures to the employees themselves);
- watching for unusual behavior by new employees or workers (e.g., workers who stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work);
- restricting access to computer process control systems and critical data systems to those with appropriate clearance (e.g., using passwords, firewalls);
- eliminating computer access to past employees immediately upon voluntary or involuntary termination;
- establishing a system of traceability of computer transactions;
- reviewing the adequacy of procedures for backing up critical computer-based data systems;
- validating the computer security system;
- using only known, appropriately licensed or permitted (where applicable) sources for all ingredients, compressed gas, packaging, and labels;
- taking steps to ensure that suppliers and transporters practice appropriate food security measures (e.g., auditing for compliance with food security measures that are contained in purchase and shipping contracts or letters of credit);
- authenticating labeling and packaging configuration in advance of receipt of shipment;
- inspecting incoming ingredients, compressed gas, packaging, labels, and product returns for signs of tampering (e.g., abnormal powders, liquids, or odors) or counterfeiting (inappropriate product identity, labeling, product lot coding or specifications), where appropriate evaluating the utility of testing incoming ingredients, compressed gas, packaging, labels, and product returns for detecting tampering or criminal or terrorist activity;
- requesting locked and sealed vehicles/containers/railcars, obtaining the seal number from the supplier, and verifying upon receipt - make arrangements to maintain the chain of custody when a seal is broken for inspection by a governmental agency;
- establishing quarantine and release procedures;
- reconciling the amount received with the amount ordered and the amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt supervising off-loading of incoming ingredients, compressed gas, packaging, labels, and product returns;

- alerting local law enforcement about evidence of tampering or counterfeiting;
- keeping track of ingredients, compressed gas, packaging, labels, salvage products, rework products, and product returns;
- investigating missing or extra stock or other irregularities outside a pre-determined normal range of variability and reporting unresolved problems to local law enforcement, when appropriate;
- destroying outdated or discarded product labels;
- securing water wells, hydrants, storage and handling facilities;
- ensuring that water systems and trucks are equipped with backflow prevention;
- testing for potability regularly, as well as randomly, and being alert to changes in the profile of the results;
- chlorinating water systems and monitoring chlorination equipment;
- maintaining contact with the public water provider to be alerted to problems;
- identifying alternate sources of potable water (e.g., trucking from an approved source, treating on-site or maintaining on-site storage);
- securing access to air intake points for the facility, to the extent possible (e.g., using fences, sensors, guards, video surveillance);
- examining air intake points for physical integrity routinely;
- keeping track of finished products;
- investigating missing or extra stock or other irregularities outside a predetermined normal range of variation and alerting local law enforcement about unresolved problems, when appropriate;
- ensuring that public storage warehousing and shipping (vehicles and vessels) practice appropriate security measures (e.g., auditing for compliance with food security measures that are contained in contracts or letters of guarantee);
- performing random inspection of storage facilities, vehicles, and vessels;
- requesting locked and sealed vehicles/containers/railcars and providing the seal number to the consignee (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes);
- advising sales staff to be on the lookout for counterfeit products during visits to customers and alerting management if any problems are detected;
- evaluating the utility of finished product testing for detecting tampering or criminal or terrorist activity;
- monitoring closely the serving of foods in open display areas (e.g. salad bars, open bulk containers);
- having a strategy for triaging the event;
- planning for emergency evacuation, including preventing security breaches during evacuation;
- identifying critical decision-makers;
- identifying management that employees should alert about potential security problems;
- identifying 24-hour contact information for local, state, and federal police/fire/rescue/government agencies;
- identifying a media spokesperson;
- having generic press statements and background information;
- identifying the person responsible, and a back-up;
- providing for proper disposition of recalled product;
- identifying customer contacts, addresses and phone numbers;
- maintaining any floor or flow plan in a secure, off-site location;
- making employees aware of internal, fire, and police emergency phone numbers;
- becoming familiar with the emergency response system and the Emergency Command Center operations in the state in which the facility is located;
- making employees aware of the company officials to alert about potential security problems, and where they can be reached;
- evaluating the lessons learned from past tampering or terrorist events;
- annually reviewing and testing the effectiveness of strategies (e.g., conducting mock criminal, terrorist or tampering event and mock recall, challenging computer security system) and revising accordingly - using third party or in-house security expert;

- performing routine and random food security inspections of facility (including receiving and warehousing areas and intrusion detection system) - using third party or in-house security expert; and
- verifying that security contractors are doing an adequate job.

Emergency Point of Contact:

U.S. Food and Drug Administration
5600 Fishers Lane
Rockville, MD 20857

If a food establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering or criminal or terrorist action, he/she should notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA District Office telephone numbers are listed at http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html. The operator should also notify local law enforcement.

COMMONWEALTH OF Kentucky Department of Education
CABINET FOR HEALTH SERVICES
DEPARTMENT FOR PUBLIC HEALTH
Developed by the Kentucky Food Safety Task Force and Food Safety Branch

FOOD SAFETY AND SECURITY INFORMATION SHEET

FOOD RELATED BIOTERRORISM, AREYOU PREPARED?

- Ensure that your facility performs pre-hiring screening of employees with background checks.
- Schedule new employees during the day shift with supervision.
- All employees should wear visible identification.
- Provide training in food security and develop a specific plan for your facility.
- Restrict personal items in food production and storage areas.
- Know your food distributor (company, driver, delivery person), and require credentials from everyone.
- Request and ensure that delivery trucks are locked or sealed between deliveries.
- Set specific times for food and product deliveries.
- Keep a log and inventory of food and product receipts.
- Keep doors leading to the outside closed and locked.
- Only authorized personnel should be allowed to enter or exit food storage, kitchen, preparation and serving areas.
- Develop a tracking system to identify lot numbers on bulk food sources that may have been recalled.
- Assign specific staff to monitor public access to buffet lines or open food areas, ensuring that foods remain safe.
- All staff must remain alert to and report signs of tampering to their supervisor.
- Have emergency water procedures available in case of contamination.
- Monitor and log food temperatures, refrigeration and cooking units.

EMERGENCY CONTACT NUMBERS: Place your local contact numbers in the chart below and post in an easily accessible place for future reference.

FIRE	
POLICE	
HEALTH DEPARTMENT	
DISASTER EMERGENCY SERVICES MANAGER/ADMINISTRATOR	
KENTUCKY PUBLIC HEALTH, FOOD SAFETY BRANCH	
UNITED STATESFOOD AND DRUG ADMINISTRATION	**502-564-7181**
	U.S. Food and Drug Administration 5600 Fishers Lane Rockville, MD 20857 If a food establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering or criminal or terrorist action, he/she should notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA District Office telephone numbers are listed at: http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html. The operator should also notify local law enforcement.